TNO innovation for life

CCE and other risk assessment methods for Industrial Systems

TNO Public | TNO 2024 R12665
19 September 2024

Author(s)	Mascha van Dort, Swarna Kumarswamy, Thomas Sierink
Classification report	TNO Public
Title	TNO Public
Report text	TNO Public
Number of pages	28 (excl. front and back cover)
Number of appendices	0
Sponsor	Rik van Dijk
Project name	NCSC Programma 2024
Project number	060.59354

Contents

1 Introduction

In the design of cyber physical systems in Operational Technology (OT), safety is paramount. A system should be designed so that the chance of an incident is minimized. Should something occur, then during an incident the impact of disruption or failure is minimized.

OT describes systems or devices that manage or interact with physical processes. These systems involve a tight coupling between the physical and computational elements, allowing them to interact in real-time and adapt to changing conditions. OT systems have increasingly integrated with ICT systems in recent years. This integration has heightened the risk of cyberattacks that could jeopardize critical industrial operations. Additionally, many OT components are aging, leading a lower quality of support and maintenance, increasing its vulnerability, and these components are more and more connected to the internet, thereby increasing the attack surface.

Consequence-driven Cyber-Informed Engineering is a methodology focused on securing the nation's critical infrastructure systems, such as OT systems [1]. In the USA, research institutes have started working with this method [2], which assumes that an attacker is skilled enough to compromise an OT system and cause damage. It is unknown whether this method or similar methods are being used in the Netherlands to increase cyber resilience.

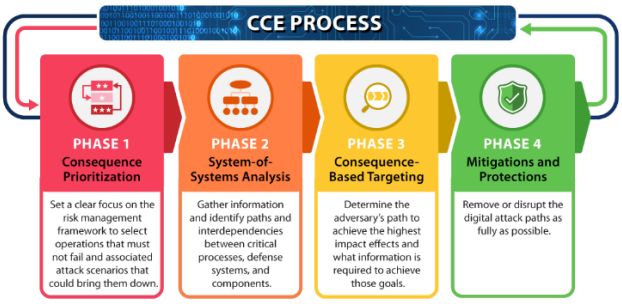

Figure 1 Consequence-driven Cyber-Informed Engineering. [1]

One problem that CCE addresses is the tendency to add security to systems at the last minute or as an extra layer applied after the systems have already been built and put into use. This tendency causes any weaknesses to only come to light after the systems are already operational. This can mean that expensive and drastic measures must then be taken to correct these errors and make the systems safer.

This document investigates to what extent the CCE methodology and other risk assessment methods of critical infrastructure can contribute to reducing cybersecurity risks in Dutch operational technology (OT) environments. Specific attention is given to the integration of CCE with methodologies within the contexts of machine safety and reducing risks in OT environments, with a focus on the design process.

For this, the following research questions have been formulated:

1. Why is it important to implement a cybersecurity strategy for OT environments?
2. What are the advantages and disadvantages of CCE and other methods for reducing cybersecurity risks in the It and OT systems of OT organizations?
3. Do organizations that operate OT systems in The Netherlands use CCE or similar methods in the design of their systems?
4. In what ways is CCE used within organizations, and which methods are mentioned as viable alternatives?
5. Can CCE be combined with methodologies used for machine safety?
6. What are viable strategies to reduce risks in OT, and how does this fit within a CCE approach?

The report scoped to OT organizations, their suppliers and the applicability of CCE. The NCSC is a stakeholder, interested in what ways they can support this upcoming domain. To investigate this, this report explored security engineering methods and cybersecurity methods and frameworks such as CCE, NIST CSF combined with NIST SP 800-82, CyHAZOP, NIST RMF combined with NIST SP 800-82, I&C systems in nuclear power plants and BSI ICS [3].

2 Approach

To successfully conduct the research, a three-step approach was selected. The first step involved a literature review, focusing on examining existing methods to enhance cyber resilience and comparing their pros and cons. The second step included in-depth interviews, incorporating an inventory of methods used in The Netherlands. Additionally, the integration of CCE with other engineering methodologies was explored. After analyzing the interview results, potential ways to mitigate risks in OT and how these fit within a CCE framework were considered.

The research started with reviewing the documentation from Idaho National Labs regarding CCE and other methods, such as NIST CSF, CyHAZOP. NIST RMF, I&C systems in nuclear power plants and BSI ICS. The literature review examined the advantages and disadvantages of the different methods. Attention was also given to the pros and cons of incorporating cybersecurity risks during the design phase compared to risk assessment after the design phase was completed. The literature review further served to prepare the interview protocol for the in-depth interviews.

Afterwards, in-depth interviews with eight (suppliers of) OT were conducted. The interviews delved into the use of CCE and other security by design methodologies, experiences with their use, results, and the need for improvement or innovation regarding these methods.

After analysis of the results of the interviews, possible ways to reduce risks in OT and how these fits within a CCE approach were considered.

Originally, an analysis of a Dutch case was planned to research the added value of the CCE methodology. However, due to time constraints and shifting priorities, the case study was omitted.

In this approach, five results were aimed for:

1. A substantiation of the importance of a (cyber)security *cybersecurity strategy for OT environments.*
2. A comparison of the advantages and disadvantages of methods in the field of (cyber)security of OT systems.
3. An overview of CCE or similar methods used the design of systems of organizations that operate OT systems in The Netherlands.
4. Insight into viable ways to reduce risks in OT and how CCE helped in this regard.
5. Tips and recommendations to promote the introduction and use of CCE in the Netherlands.

3 The importance of a cybersecurity strategy for OT environments.

In an analysis of incidents between 2020-2023 cybersecurity in OT was assessed. Over this period, the number of publicly reported attacks on industrial systems per year doubled [4], as can be seen in Figure 1.

From 2020 to 2023, the energy sector was frequently targeted by cyber incidents, primarily by organized groups and nation-state actors. Both IT and OT environments were attacked, with a notable rise in dual IT/OT attacks. The water sector also saw an increase in cyber incidents, reflecting the impact cyber incidents can have on public health and safety. These attacks were mostly carried out by organized groups and nation-state actors, targeting both IT and OT environments. The transportation sector experienced steady cyber incidents, mainly by organized groups, as they rely on OT for logistics and signaling. The healthcare sector faced consistent cyber attacks, primarily on OT or IT/OT environments. The identity of the threat actors was often unknown, raising questions about their motives.

The IT environment experienced the most successful attacks, often due to ransomware. Threat actors typically start with IT and attempt lateral movement to OT, though this wasn't always successful. Successful breaches often resulted from:

1. Use of outdated software, leading to vulnerabilities due to compatibility and support issues.
2. Lack of Multi-Factor Authentication (MFA) and inadequate protection of login credentials and access.
3. Use of remote access software like TeamViewer, which, if not properly secured, provides entry points for attackers.
4. Network segmentation could have prevented some attacks by containing them to limited areas, preventing spread to other parts of the network.
5. Human errors, such as compromised user credentials stored in personal cloud services or leaked on the dark web.
6. Insufficient basic cyber hygiene in Industrial Control Systems (ICS), with publicly exposed systems and networks being easy targets.

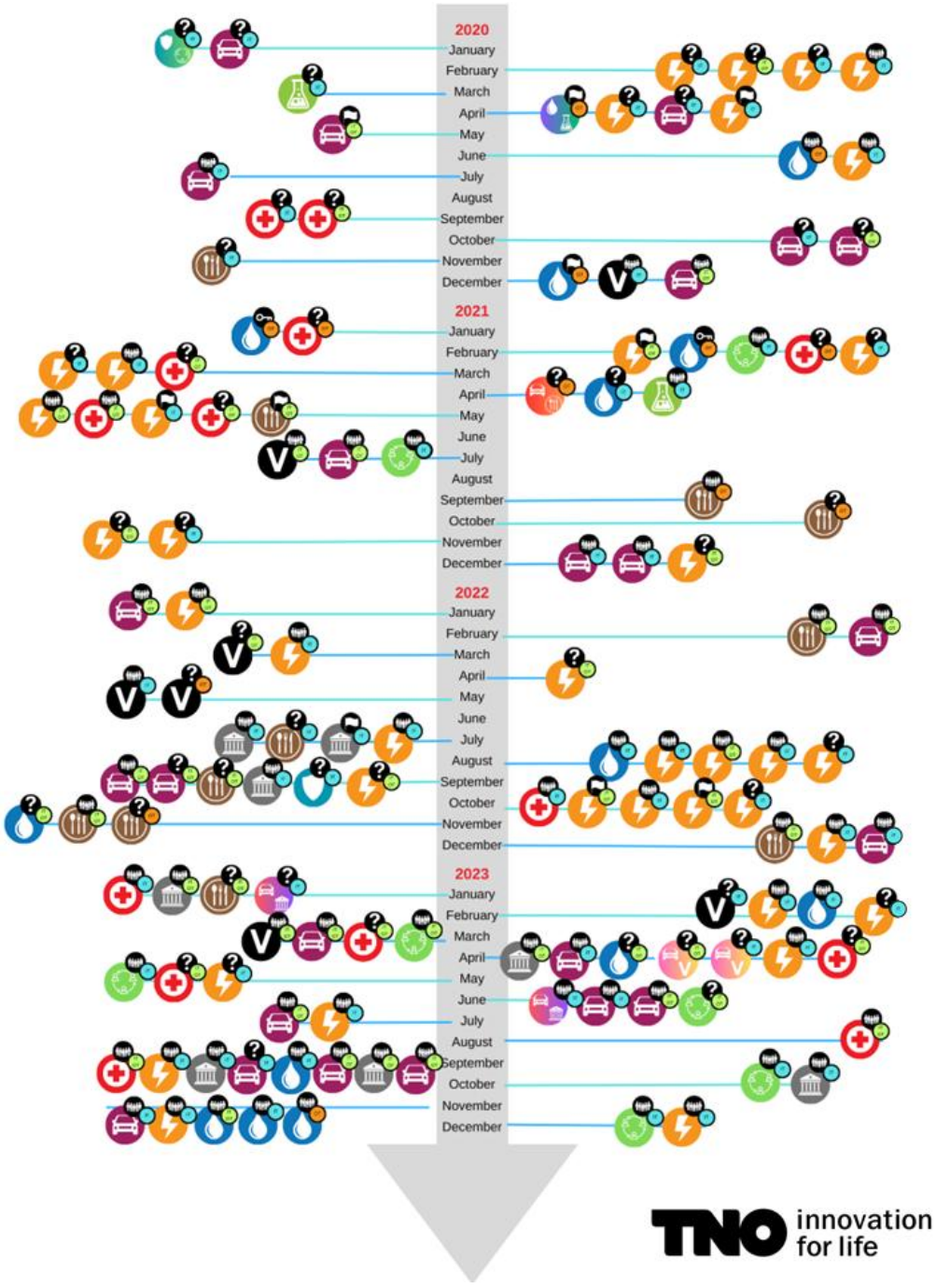

Figure 2 Timeline of 2020-2023 Industrial Systems Incidents.[4]

Type of Attacks varied. From 2020 to 2022 it was mostly ransomware attack varieties. While DDoS became more prevalent in 2023.

The consistent targeting of critical sectors like energy and water, by organized and state sponsored groups highlights the need for ongoing adaptation in security strategies. A structural approach to risk management such as Consequence-driven Cyber-Informed Engineering (CCE) or similar methods could provide viable foundations to assess and adapt security strategies.

4 Methods and frameworks for cyber security risk assessment

In this chapter, a selection of methods and frameworks is made to compare CCE alongside with. After selecting based on four metrics, the metrics are discussed, along with their differences, overlaps, advantages, and disadvantages.

An initial inventory was made based on literature and real-world use. Then, methods were selected in a second round based on four criteria:

- Does the method have components that are specific to OT and/or cyber?
- Does the method have a high applicability to various contexts and levels of complexity?
- Does the method regard a complete perspective on OT risk, including threats, impact, safety?
- How available is the method? For instance, is material available for free?

Results to these questions are displayed in Table 1. The four bold methods and frameworks are selected.

Table 1 Methods and frameworks ranked on four metrics.

Initial selection	OT / cyber specific	High applicability	Complete perspective	Availability
CCE [1]	✓	✓	✓	~
Bowtie [5] link	~	✓	~	✓
NIST CSF + NIST SP 800-82 [6]	✓	✓	~	✓
CyHAZOP [7]	✓	~	✓	x
NIST RMF + NIST SP 800-82 [6]	✓	✓	✓	✓
I&C systems in nuclear power plants [8]	✓	x	~	✓
BSI ICS [9]	✓	✓	✓	x

4.1 CCE

Consequence-driven, Cyber-informed Engineering (CCE) is a methodology designed by the Idaho National Laboratory (INL) to secure critical infrastructure systems. It assumes that an attacker can and will attack and penetrate the system. It therefore is not about vulnerability reduction, but it focuses on reducing impact of possible attacks with high consequence. Following these statements, it is important to note that CCE's purpose is not to increase enterprise-wide security posture. In this context, there a four-phase approach:

- Phase one: Consequence Prioritization;
- Phase two: System-of-Systems Analysis;
- Phase three: Consequence-Based Targeting; and
- Phase four: Mitigation and Protections

Consequence Prioritization

The primary goal of CCE is to identify and prevent high-consequence events of an organization. Therefore, the first step of the methodology asks to identify High-Consequence Events (HCEs) that could potentially halt critical services and functions. These events typically have physical consequences. From these events, CCE focuses solely on events caused by cyber methods. Then, the severity of these events should be determined by a set of predefined factors. The INL suggests:

1. Area impacted
2. Cost for recovery
3. Public safety
4. System integrity
5. Attack breadth
6. Duration

Given the context, the HCEs should now be determined through expert dialogue and their severity scored through the earlier created factors. For this, organizations must assume the attacker's success.

System-of-Systems Analysis

For each HCE, a high-level block diagram should be created, depicting what information and access an adversary requires to accomplish the HCE. It should include technologies, processes, and people. This information should then steer data collection actions. The detail of this data collection should be high, and the process iterative. Combining the high-level diagrams and the collected data, system diagrams are created which include a logic diagram, connections diagram, and a network diagram. From this follows a systems-of-systems summary, over which a review of subject matter experts is performed.

Consequence-Based Targeting

Phase three aims to find places with unverified trust. Combining the first two steps, a high-confidence kill-chain should be developed and validated. This is done though identifying the technical target and describing the technical approach. Thus, creating an attack scenario, also referred to as Scenario Concept of Operation (CONOPs). The absolutely necessary information to execute this attack is then recorded. This information is then deemed as top-critical.

Mitigation and Protections

The final phase focuses on the identification and development of possible protection strategies, mitigating the kill-chains and CONOPs. These are first brainstormed, mapped and prioritized, and then validated. Leadership is then expected to define next steps. A last step to this final phase is the development of adversary tripwires. Think of increased or specific detection capabilities, or techniques as honey pots and the like, potentially providing information on the current status of mitigations and edge cases.

4.2 Bowtie method

Bowtie diagrams (Figure 2) are a popular way to perform risk analysis. Using this method, a Bowtie diagram is used to visualize risks with a clear differentiation of proactive and reactive steps [10]. To perform this analysis these steps are followed:

1. Hazard – the start of a Bowtie analysis begins with a hazard to an organization, which has the potential to cause any damage.
2. Top-event – Once a hazard is chosen, a top event is considered from this hazard. This top event is chosen before it can start causing any potential damage.
3. Threats – These are any actions which can directly lead in causing the top-event. Being specific here will help in providing a complete picture for the risk analysis.
4. Consequences – Finally consequences can be added as results from a top-event. There can be multiple consequences linking to a single top-event.
5. Barriers and escalation factors – In order to prevent threats from happening and mitigating consequences, barriers can be set in place. The failure of a barrier is described in an escalation factor.

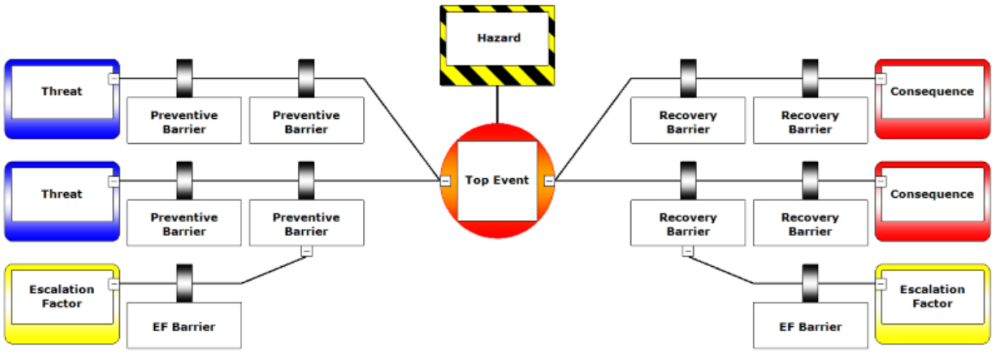

Figure 3 Bowtie diagram with descriptions of sections.

Although the Bowtie methodology for risk assessment is not focused on cybersecurity, nor on OT risks, it can be applied in these situations. With reference to a paper published in 2019 [11], this method was used to perform cybersecurity risk analysis along with their Risk and Opportunity Based Asset Management process at Dutch DSO (distribution system operator) Enexis. In conjunction with IEC62442/3 guidelines a risk assessment was made.

Furthermore, in recent studies Bowtie methods have been combined with other methods for risk assessments particularly in the cybersecurity areas to combine both safety and security risk assessments [5]. Traditionally, Bowtie methods have been used keeping safety in mind. But with the increase in digitization in all areas, OT systems are no longer air-gapped or isolated which leads to new threats and vulnerabilities with increased connectivity, which will certainly have an impact on safety of OT systems. Hence it is needed to have a complete view while performing risk assessments of entire system, system of systems.

4.3 RMF + NIST SP 800-82

Fundamentally, the Risk Management Framework (RMF) by NIST does not have a focus on OT cyber risks. The RMF is a general risk management framework that any organization can use for managing their information and privacy risks. However, with Special Publication 800-82, the RMF received OT-specific guidance, making it highly applicable for OT.

Every step in the framework is comprised of several subtasks, allowing for a complete and detailed execution of every step.

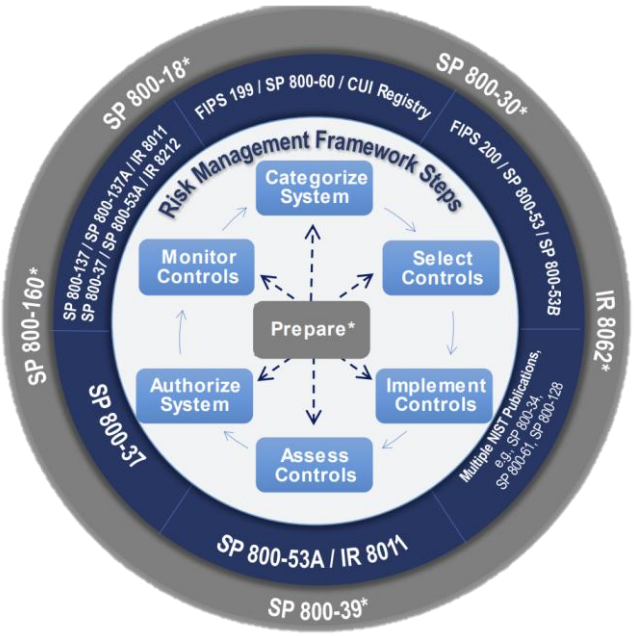

Figure 4 The steps of RMF.

Prepare

The prepare step is performed to support all further steps of the RMF. It is divided in two levels, the organizational and the system level. On both levels, risk management roles and strategies should be developed. Per level, a risk assessment should be performed. This risk assessment should be followed through NIST's CSF. The Identify step herein contains instructions for a risk assessment. In short, it urges to find vulnerabilities in assets first, after which threats exploiting these vulnerabilities are weighted on impact and likelihood. Then, risk responses are selected, and potential changes managed.

Categorize

First, the characteristics of a system should be described. Then, based on the three security objectives, confidentiality, integrity, and availability, the impact levels should be determined for every information type and system. Availability is usually of the greatest concern in OT systems.

Select
In the select step, initial security controls are selected that are necessary to protect the system. These baselines can be tailored per system. Finally, a continuous monitoring strategy to these controls must be implemented.

Implement
Security controls are implemented and documented. A distinction is made between new systems and legacy systems. In the case of the former, the implementation takes place in a requirements definition perspective. The latter case requires a gap analysis perspective.

Assess
The assess step aims to determine to what extent the controls are effective in their use and whether they produce the desired results. This is done in accordance with security and privacy assessment plans. Any unacceptable risk is an insufficient result and is remediated through a remediation plan.

Authorize
After having produced and assessed the revised system, management should decide on the operation of the system, accepting the risks to operation, assets, and people involved in the implementation of the discussed set of controls.

Monitor
The final step continuously tracks any mutations to the system that could lead to changes in control effectiveness.

4.4 BSI ICS Cybersecurity Assessment Framework

The BSI ICS Cybersecurity Assessment Framework combines useful components from several standards and methods: ISA/IEC 62443, ISO27001, NIST, CPNI, and ENISA. The eight steps to follow are as follows.

Current state definition
Define the current state of the OT control system. Gather all relevant information and assets to perform a risk assessment.

Target state definition
The target state definition defines which cyber security controls, processes and procedures should be in place for both OT and IT. This involves communication between IT, OT, physical security and HR to agree on controls.

Gap analysis
There should be a continuous process of gap assessment between the current and target state, as the current state and its surroundings is everchanging where new priorities might come into play.

Creating threat profile
Having a clear idea of threats is important. Per 'gap', corresponding threats can be explored. Moreover, the framework sees threats not as separate events but wants to view combinations of threats leading to highly successful attacks. The threat profile contains vulnerability, exploit, threat, threat actor, threat scenario, and threat scenario campaigns.

Risk analysis
In risk analysis, risks are first identified. What zones of the system are influenced, and who are the stakeholders? Their impacts are then ideally qualitatively and quantitatively determined. The framework does not prescribe through which method this should happen. However, with quantitative influences on impact and likelihood, risk priority can be determined. Finally, they can be grouped in a risk heatmap for overview.

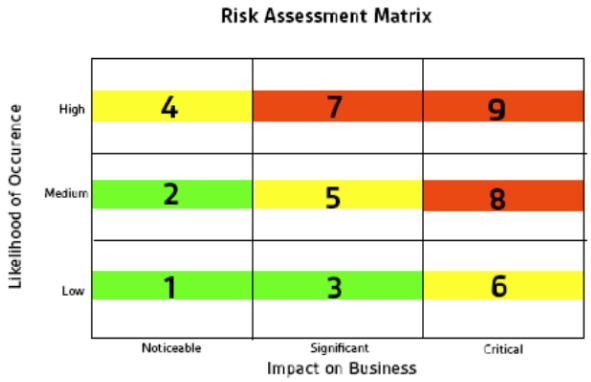

Figure 5 BSI ICS Cybersecurity Risk Assessment Matrix.

Remediate
Per identified risk and prioritization of these, an appropriate remediation has to be thought of. The framework suggests following one of ISO27001's remediation strategies (transfer, accept, treat, and avoid), while keeping in mind to keep the scope to each of IEC 62443's element groups (people, processes, technology).

Benchmarking
Rather than yes/no-benchmarking, running over a checklist, this framework proposes to not only check the recommended controls, but also go over the threats and threat scenarios, to see what residual risk is left.

Program maturity
As a last step, the framework recommends introducing an organization-wide cyber security management system. This keeps a continuous management program going, preventing analyses being seen as temporary projects.

4.5 Comparison

Within several themes, overlaps and differences between the frameworks can be observed.

"Where do I even begin" – how much guidance is given up front?

When performing risk assessments and applying risk reduction methods, the start can be difficult. The discussed frameworks and methods have a varying degree of guidance to start off with. The first step of CCE urges to think of the events that affect your organization or their mission the most, HCEs. For this, it is assumed that any vulnerabilities present definitely will be exploited. The Bowtie method is similar to the above yet does not offer specific guidance on how to pursue a first collection of hazards or corresponding events. Furthermore, it shares the assumption that vulnerabilities will be exploited: the threats and escalation factors collected are not chosen based on likelihood. The objective remains therefore clear, although scoping is missing. BSI starts off with the gathering of the information of all assets: their cyber security controls, processes and procedures are all collected. Then, a target state of how these characteristics ideally should be is created. The difference between the current state and target state is the 'gap'. Important to note is that a risk within gap analysis is that it assumes the target state to be fully secure. Assuming that there exists no secure state by assuming breach, as what CCE does, would solve this.
The RMF starts off with the collection of all vulnerabilities in all assets. Then, the threats exploiting these vulnerabilities are weighted on impact and likelihood. Apart from the low feasibility in this task, this goes directly against CCE where the likelihood of every vulnerability is seen as a 100% chance.
As a part of the first step, we observe a difference in perspective between the methods: event-based vs asset-based.

Event-based versus asset-based

Where CCE and Bowties are event-based, the RMF and BSI framework are asset-based. The event-based methods start off with high impact events and collect connected assets to these. The asset-based methods collect all assets to then create a picture of what impact can be created should these be exploited given some likelihood.
IEC 62443 recommends that whichever approach is followed, some aspects of one approach should be included in the other to provide a more thorough risk assessment. There is a clear distinction which of the two approaches to favor, depending on the organization assessing their risks. An event-based approach does not want to limit all existing vulnerabilities. It might even be that some vulnerabilities might be left undiscussed or even unnoticed, simply because they do not lead to high impact events. You might find this style of approach in critical infrastructure where operation must continue, despite a breach of security. Asset-based approaches first regard all assets, systems, and processes. This desire to be complete could prove to be difficult, (equally as for asset gathering in event-based methods). For organizations with a high desire of protecting the information they own, any breach could already lead to an impact. Vulnerabilities are much more crucial. Furthermore, some organizations might find their image damaged when a breach occurs – even if the breach itself caused no impact.

Way of prioritizing

The prioritization of which risks to address first can be of great help in complex systems. As for being a simple method and not having risk management components, Bowties do not inherently prioritize risks. Given expert knowledge however, Bowties could aid decision-making. In [11], likelihood was based on historical events and the barriers' strength were based on expert judgement. As mentioned earlier, CCE suggest six factors based on which a priority ranking can be created. Other factors can also be used, and the weights per 'metric' should be determined by the assessors. The RMF bases priority on the CIA-triad and severity within those: a very cyber-known concept. The BSI Framework has no prescribed way of defining impact or likelihood, but using a risk assessment table based on impact and likelihood a priority may be inferred.

Threat modeling

CCE aims by identifying the target and describing the approach of attack to create an attack scenario, also referred to as a scenario Concept of Operations (CONOP). All information that comes forward to be absolutely necessary in the successful executing of this attack is then recorded. Based on this information, mitigation can then take place.
The BSI framework recommends creating a threat profile containing vulnerability, exploit, threat and threat actor. Together, this can be used to form a threat scenario. This is then effectively the basis of the kill chain – thus formed by thinking like the attacker – which needs to be mitigated.
The RMF and Bowties don't model threats or scenarios specifically. While the Bowtie method has threat components on its left side, these are not quite models or detailed scenarios. However, these threats could be used in combination with a threat scenario towards a solid risk assessment. Moreover, one could argue that having created a Bowtie diagram, it could be used as a blueprint for a kill chain. Furthermore, as the RMF suggests using the CSF for risk assessment and identification, it should be mentioned that the CSF recommends to get an overview of threats, but does not elaborate further.

Determining mitigations

Also, the mitigation of risks is performed differently per method. CCE regards the attack kill chain and recommends seeing what can be done to 'break' the kill chain and make the objective of the attacker unavailable. Furthermore, CCE suggests the installation of 'tripwires' in the system to help detection and understand attacks. The Bowtie approach is similar to CCE, where barriers or escalation factor barriers are created to break the possible outcomes in the 'fault tree' from happening. In the RMF, initial security controls are selected that are necessary to protect the system, based on gap analysis for legacy systems, and based on development requirements in new systems. These controls are then implemented and documented. Lastly, the BSI framework suggests following one of ISO27001's remediation strategies – transfer, accept, treat, and avoid – while keeping in mind to keep the scope to each of IEC 62443's element groups (people, processes, and technology), but does not give any guidance on which to follow.

Continuous assessment built-in

Given the context of cyber security with ever-changing threats and vulnerabilities, it is of importance that assessment is not a one-time occasion but is a continuous activity.
CCE and Bowties lack this inherent continuous assessment. Their application could be made a part of an ongoing process, but the methods themselves do not facilitate this.
On the other hand, BSI suggests setting up a cyber risk management program, to make these assessments a continuous occupation. Also, the gap analysis should be performed continuously. RMF also recommends to continuously monitor changes to the system or its surroundings to adapt if necessary.

General remarks

Whichever framework or method is applied, there is always a chance of incompleteness and a big reliance on expert knowledge in every framework/method. Moreover, based on the varying types of frameworks, the approach to follow differs greatly per organization based on size, maturity, and focus. Also, it remains to be tested whether the end results of conducting two different methods differ in a meaningful way.

5 Interview findings

We have conducted several interviews with experts from diverse organizations working in operational technology. These interviews were conducted to provide insights on how risk assessments are performed while taking into account both cybersecurity and safety aspects.

Context of interviewees

The interviews we conducted represented sectors of energy, transport and mobility, product manufacturers specialized in PLCs[1] and high-tech industry. This represents a diverse set of industries with operational technology which gives a good insight related to cybersecurity and safety while looking at risk. The interviewees had different functions such as CISO, business director, product and solutions security expert, and technical officers. In their roles, they had an overview of risks involving both cyber security and machine safety. While representing machine safety it was also noted that in many organizations this was categorized into Health, Safety and Environment.

Overview of CCE or similar methods used in the design of systems of organizations that operate OT systems in The Netherlands

With the aspect of their current practices on risk assessment, several interviewees were using the standards from IEC 62443. This was further customized to their organization needs and based on experiences from the field. Some of the organizations, used Bowties for assessing high-impact incidents and risk assessments. Certain organizations also use ISO 27001 in combination with IEC 62443. One organization has developed their own methodology based on threats, vulnerabilities and impact. This was further elaborated mapping vulnerabilities to assets and impact to events. The ISO 27001 and IEC 62443 series of standards complement each other. ISO 27001 deals with security management for the entire company, while IEC 62443 focuses on security concepts for industrial control systems. However, their focus on cyber risks for OT is small. Risk approaches in use are performed with two types of assessments, namely event-based or asset-based. Another key aspect which was mentioned during the interviews was business continuity. There are clear overlaps between event-based risk methods and such business continuity, for instance that they both focus on the operational functionality of the process.

[1] A Programmable Logic Controller (PLC) is a specialized computer used in industrial and manufacturing processes to control machinery and equipment. PLCs are designed to automate industrial processes, such as assembly lines, robotic devices, or any activity that requires high reliability and ease of programming and process fault diagnosis. A typical PLC consists of a processor (CPU), memory, input/output (I/O) modules, and a power supply. The CPU executes control instructions based on the program stored in its memory. PLCs are programmed using specialized languages, with Ladder Logic being one of the most common. These languages are designed to be easy for engineers and technicians to use. They can be reprogrammed and reconfigured to adapt to different tasks and processes, making them highly versatile. PLCs are built to withstand harsh industrial environments, including extreme temperatures, humidity, and electrical noise.

Table 2 Reported Cyber Security risk assessment methods used per organization.

Method	Mentioned
IEC 62443	4
Own method	3
ISO27001	2
Bowtie	2
CCE	0
RMF + NIST SP 800-82	0
BSI ICS Cybersecurity Assessment Framework	0

Although a small sample of OT organizations, the interviews revealed a lack of standardization in the use of methods for risk assessments, with no extensive rationales provided by interviewees regarding their choices, timing, or frequency of use. Much of the decision-making was left to the discretion of the Chief Information Security Officer (CISO), resulting in varying levels of structural approaches across organizations. A significant issue identified was the lack of dedicated and trained expert staff to carry out these assessments, underscoring the necessity for experts with comprehensive knowledge to perform thorough risk evaluations. This also points to a lack of attention from management to hire or train such personnel.

Familiarity with CCE

None of the interviewees were familiar with CCE before receiving the invitation to the interview. This lied within the expectations: CCE is not a widespread methodology. However, several interviewees have remarked to have a strong familiarity with multiple aspects of the framework. This recognition came in different degrees. One interviewee completely saw their own way of working formalized into a framework. Some other interviewees recognized broadly the same topics they work within the framework. For example, one interviewee found that CCE is very comparable to business continuity frameworks and did not see much novelty. There were no responses of unfamiliarity surrounding the concepts discussed.

Initial evaluation of CCE

Of the seven interviewees, all agree to varying extents to the statement that the CCE approach falls in line with what they experience as necessary for risk assessment in OT. Across all interviewees, there was no response that found the approach significantly novel. On several aspects, there are considerations concerning the framework regarding applicability in the interviewees' context. Their remarks are summarized below.

The first aspect of CCE that yielded interesting comments was the fact that CCE is event-based. In order to create High Consequence Events, you are required to at least have baseline knowledge of what assets are relevant to the context. This is a manager-like perspective. That is, from a high-level perspective the assets need to be incorporated in the process.

Conversely, another interviewee remarked that event-based might work high-level, but in the end we talk about low-level assets that are required to build (and break) attack chains. If we need to incorporate assets anyway, we need to be complete. Another interviewee shares this view, stating that it is very possible to miss something. It is therefore difficult to be complete without working asset-based. A solution might be to have an asset list in the background during the process. Lastly, a notable remark is that the CCE method is seen as doable per asset, but costly if performed on a system level.

The second theme is the use of impact in HCEs. It neglects to consider likelihood since the framework assumes breach. Yet some interviewees remarked that for different types of companies, the likelihood does matter. For instance, when a company has a sensitive public position, relies on trust, sees its image as crucial, or has stocks that can be impacted by an incident. Furthermore, some organizations are fine with accepting risks. Not every risk that has great impact is worth spending money on if its likelihood is very small. The finance dictates to a certain extent the risk appetite.

Lastly, some interviewees understood CCE to represent a method, not a (iterative) process. For them, it sounds like a technology development method where iteration is not inherently part of the process compared to other existing frameworks. They see it as something to integrate with their existing structures. Overall, interviewees saw that there is no single standard that solves all intricacies of their risk context. Combining components of different standards and taking inspiration works best. And on top of that is that all standards rely on expert opinions, which all interviewees underline.

Although combining standards and methods to best fit the context can be beneficial, it also highlights the ongoing issue of a lack of standardization in risk assessment methods. Interviewees did not provide extensive rationales for their choices, timing, or frequency of use. Implementing a standardized, structural approach would offer a baseline with a clear rationale in the Netherlands, which could then be expanded to incorporate multiple methods.

Combination of CCE with methodologies used for machine safety

To combine both cybersecurity and machine safety, we can turn our attention to IEC 62443, being a widely used and customized standard for risk assessment. The high adoption among the interviewees is a symptom of this. The standard claims that industrial control systems that are not designed with cyber security in mind may have health, safety and environmental (HSE) consequences. Over the whole, the standard has an elaborate description of measures to take to prevent impact, be it in terms of safety or otherwise. However, looking at a machine safety, standards like the IEC 62061 (Safety of machinery - Functional safety of safety-related control systems) or the ISO 12100 (Safety of machinery - General principles for design - Risk assessment and risk reduction) should be adhered when relevant. These have a are safety-first vision: “The present philosophy in IEC 62061 considers that security has to be considered in safety-related control systems. It requires that security

measures should not have an adverse effect upon safety.", as a guiding statement of the IEC 62061 update says.[2] The ISO 12100 in turn is complemented by ISO 22100-4, which provides guidance to machinery manufacturers on considering cyber security aspects that can influence machine safety.[3] However, this standard has a broad IT-security view. The ISO standard "provides essential information to identify and address IT-security threats which can influence safety of machinery."

It should therefore be advisable that these standards require a framework or methodology like CCE to gain a stronger focus on OT security, while these safety frameworks are essential to ensure that safety is not hampered by security.

[2] https://etech.iec.ch/issue/2021-02/updated-iec-standard-ensures-the-functional-safety-of-machinery
[3] https://www.iso.org/news/ref2365.html

6 Conclusions and recommendations

Between 2020 and 2023, the number of publicly reported cyber attacks on industrial systems doubled. The energy sector was frequently targeted by organized groups and nation-state actors, with both IT and OT environments being attacked. The water sector also saw an increase in cyber incidents, impacting public health and safety. The transportation and healthcare sectors experienced steady cyber attacks, primarily on OT or IT/OT environments. The consistent targeting of critical sectors highlights the need for ongoing adaptation in security strategies. This research investigated whether Consequence-driven Cyber-Informed Engineering (CCE) or similar methods could provide viable solutions.

Consequence-Driven Cyber-Informed Engineering (CCE) is widely recognized in interviews as an appropriate method for conducting tabletop risk analyses. Although organizations may not be familiar with CCE specifically, they are acquainted with similar methods. Many interviewees recognized aspects of the framework from their own practices. For example, IEC 62443 is a widely used and customized standard, also offering a risk assessment framework in Part 3-2. The CCE approach is considered to contain the most important steps and is therefore considered very appropriate by those interviewed. Therefore, we believe it is a suitable approach for organizations that operate OT technology and systems. However, its actual employability does vary for different types of organizations. To support this further, the CCE method is discussed per step.

Viable ways to reduce risks in OT with asset based and/or event based (CCE)
As a result from comparing similar methods and frameworks in Chapter 3, two primary strategies of risk analysis methods were identified: asset-based risk analysis and event-based risk analysis. Event-based methods, such as Consequence-Driven Cyber-Informed Engineering (CCE) and Bowtie, focus on high-impact events and their subsequently related assets. In contrast, asset-based methods like the Risk Management Framework (RMF) and the BSI framework start with gathering all assets and assess potential impacts that arise from those.

In short, this means that CCE begins with identifying high-consequence events (HCEs), assuming all vulnerabilities will be exploited. The Bowtie method is similar to CCE but lacks explicit guidance on initial hazard collection. The BSI framework starts with gathering information on all assets and identifying gaps between current and target states. RMF collects all vulnerabilities and assesses threats based on impact and likelihood, contrasting with CCE's assumption of 100% likelihood for vulnerabilities.

Taking a step back, IEC 62443 recommends incorporating aspects of both approaches for a thorough risk assessment. It is advisable to combine good aspects from various frameworks, balancing asset and event considerations. All frameworks rely on expert knowledge and may have gaps. The choice of approach depends on the organization's context and size, as shown in Table 3.

Table 3 Recommendation of event-based or asset-based methods for varying types of organizations.

Organization type	Recommendation	Reason
Organizations with high public sensitivity or regulatory requirements	Focus on event-based methods initially, with a strong emphasis on high-consequence events	Prioritize high-impact events that could affect public image or regulatory compliance
Critical infrastructure organizations	Prioritize event-based methods but ensure asset-based assessments are not neglected	Crucial to identify and mitigate high-impact events to ensure operational continuity
Organizations that are neither of the above	The use of either type can be beneficial. Use the method that aligns best with your needs and be aware that a hybrid approach might suit best.	For smaller organizations, it might help to start with an event-based method that guides the identification of risks. Larger organizations could choose to spend more resources on asset-based methods.

CCE's strongest asset also contains its biggest risk: the initial step of inventorying high-consequence events. Cybersecurity maturity levels in OT organizations vary significantly. Organizations with lower maturity levels may lack technical judgement to value high-consequence events correctly. Therefore, if the method is applied by a team with insufficient maturity, the initial step may yield suboptimal results. Moreover, in some OT organizations, cybersecurity measures are given low priority by asset managers, during short maintenance downtimes, often because of an operational focus, as any downtime can have significant financial and safety implications. Moreover, many OT environments rely on older, legacy systems. Upgrading those systems can be costly and complex. Also, there can be a lack of awareness or understanding of the cybersecurity risks specific to OT environments among asset managers. In the interviews we heard that penetration testing in operational environments is frequently limited due to potential operational consequences. As a result, the lack of penetration testing may lead to asset managers being less aware of cybersecurity risks and priorities.

To overcome these hurdles, it is recommended that the National Cyber Security Centre (NCSC) organizes a team of experts with the ability and specialty in thinking up worst case scenarios that may occur of OT systems and processes are breached: visiting CISO teams of more mature OT organizations to assist in step 1 of CCE. The primary value of performing such a tabletop exercise lies in achieving a shared awareness of the need for cybersecurity investments and prioritization among asset managers and cybersecurity personnel. Many interviewees noted that this shared understanding is currently lacking. This is most effective

when all necessary internal stakeholders, including cybersecurity personnel and asset managers, are involved.

To conduct effective tabletop exercises, it is crucial to include a diverse group of participants such as risk managers, cybersecurity experts, and an external team of visiting CISO teams of more mature OT organizations to assist in step 1 of CCE to ensure a comprehensive perspective. CCE's event-based nature requires baseline knowledge of relevant assets, which can be challenging without an asset-based approach. A suggestion is to maintain an asset list in the background.

To support the diverse background of participants, cybersecurity experts should illustrate all potential scenarios and attack paths in step 3, providing clear visualizations for those who may not be familiar with cyber risks. A suggestion is to use table printouts of the MITRE attack framework to visualize attack paths. This inclusive stakeholder approach helps in fostering a shared understanding and prioritization of cybersecurity measures within the organization. Conducting step 4 together ensures that asset managers are involved to secure buy-in for necessary investments.

There are some considerations regarding step 4 in the CCE method. Currently, step 4 strongly advocates for the mitigation of *all* high-consequence events, regardless of their likelihood of occurrence. This might not be valid for all sectors or organizations. Moreover, the use of impact in High Consequence Events (HCEs) without considering likelihood was seen as a limitation by some interviewees, since likelihood matters for companies who want to accept certain risks for financial reasons. We therefore suggest the following approach to ensure a balanced, cost-effective and efficient step 4 approach:

Table 4 Recommendation of incorporating likelihood in mitigation decisions for varying types of organizations.

Organization Type	Recommendation	Reason
Organizations with high public sensitivity or regulatory requirements	Focus on HCEs without likelihoods	Prioritize high-impact events that could affect public image or regulatory compliance
Critical Infrastructure Organizations	Focus on HCEs without likelihoods	Crucial to identify and mitigate high-impact events to ensure operational continuity
Organizations that are neither of the above and/or have limited resources	Focus on HCEs but take your risk appetite in consideration. Depending on the organization's size and financials, some HCEs can be accepted.	A realistic vision can be applied if the organization does not situate itself in sensitive contexts.

Tips and recommendations to promote the introduction and use of CCE in the Netherlands.

Interviews highlighted the ongoing issue of a lack of standardization in risk assessment methods (See page 23-24). Interviewees did not provide extensive rationales for their choices, timing, or frequency of use. Implementing a standardized, structural approach would offer a baseline with a clear rationale in the Netherlands, which could then be expanded to incorporate multiple methods.

We recommend CCE as a risk assessment methodology for critical national infrastructures additionally using likelihoods in step 4, and recommend to organizations with high public sensitivity or regulatory requirements to use standard CCE's approach. Although all other sectors could profit of a more standardized approach, we suggest leaving that open, and to promote the use of regular standardized risk method, either event-based or asset based (see tables 3 and 4). Training should be offered to support the standard. Besides that, all organizations operating in an OT environment are recommended to follow standards providing security guidelines, of which we can recommend IEC 62443. Where machine safety is relevant, IEC 62061 can be of use. Having these standards in place, CCE can act as an iterative, recurring assessment method that pushes the adoption of a standard's guidelines, yet can be used to find other, overlooked risks too.

To encourage best practices like conducting annual standardized risk assessments, it is recommended that the National Cyber Security Centre (NCSC) forms a team of experts proficient in CCE and worst-case scenario planning for OT systems and processes (See page 28). This team should include experienced CISOs and risk managers from more mature OT organizations. By conducting tabletop exercises with this expert team, cybersecurity awareness will be heightened, and a shared understanding of the importance of cybersecurity investments and prioritization can be fostered among all relevant internal stakeholders, including asset managers and cybersecurity personnel. This will promote both cyber security awareness as well as a more standardized approach with highly trained experts ensuring self-organization and resilience of the OT sector.

7 References

[1] A. Freeman and S. Bochman, Countering cyber sabotage: introducing consequence-driven, cyber-informed engineering (CCE), Boca Raton: CRC Press, 2021.

[2] S. Freeman, N. Hill Johnson and C. St Michel, CCE Phase 1: Consequence Prioritization, Idaho Falls: Idaho National Laboratory, 2020.

[3] M. Ernie Hayden and CEH CISSP, Critical infrastructure risk assessment: the definitive threat identification and threat reduction handbook., Brookfield: Rothstein Publishing, 2020.

[4] R. Ibis and R. Ibis, Cyberattacks on Industrial Control Systems between 2020-2023, The Hague: TNO, 2024.

[5] H. Abdo, M. Kaouk, J.-M. Flaus and F. Masse, "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis," *Elsevier Computers & Security,* vol. 72, pp. 175-195, 2017.

[6] NIST, *NIST SP 800-82r3,* NIST, 2022.

[7] TÜV Rheinland, *CyHAZOP – Bringing cyber to the HAZOP,* 2022.

[8] L. L. K. L. Song, *A cyber security risk assessment for the design of I&C systems in nuclear power plants,* Korea Science, 2012.

[9] BSI Group, *ICS Cybersecurity Assessment Framework,* 2020.

[10] W. Kluwer, "Wolters Kluwer," [Online]. Available: https://www.wolterskluwer.com/en/solutions/enablon/bowtie/expert-insights/barrier-based-risk-management-knowledge-base/the-bowtie-method. [Accessed 15 October 2024].

[11] M. Hoeve, C. Monte Portela and G. Brouns, "Managing OT cyber-security risks using bowties and risk & opportunity based asset management at Dutch DSO Enexis," in *25th International Conference on Electricity Distribution*, Madrid, 2019.